Serial No. 10/085,346   PD-200336

IN THE CLAIMS

Please amend claims 1, 6, 10, 15, 19, 24, 28, and 33 as follows:

1   1.   (CURRENTLY AMENDED) A system for controlling access to digital services

2 comprising:

3   (a)   a control center configured to coordinate and provide digital services;

4   (b)   an uplink center configured to receive the digital services from the control center

5 and transmit the digital services to a satellite;

6   (c)   the satellite configured to:

7   (i)   receive the digital services from the uplink center;

8   (ii)   process the digital services; and

9   (iii)   transmit the digital services to a subscriber receiver station;

10   (d)   the subscriber receiver station configured to:

11   (i)   receive the digital services from the satellite;

12   (ii)   control access to the digital services through an integrated

13 receiver/decoder (IRD);

14   (e)   a conditional access module (CAM) communicatively coupled to the IRD,

15 wherein the CAM comprises:

16   (i)   a nonvolatile memory component, wherein:

17   (1)   the nonvolatile memory component is used to contain state

18 information to provide desired functionality and enforce one or more security

19 policies for accessing the digital services; and

20   (2)   the nonvolatile memory component is protected from

21 modification such that the nonvolatile memory component is read only; and

22   (3)   access to the nonvolatile memory component is isolated;

23   (ii)   a hidden non-modifiable identification number embedded into the

24 nonvolatile memory component, wherein:

25   (1)   the identification number uniquely identifies the CAM; and

2

Serial No. 10/085,346   PD-200336

26   (2)   the identification number is used to limit a cloning attack wherein

27   said cloning attack comprises copying the identification number to a new CAM;

28   and

29   (iii)   a fixed state custom logic block, wherein the nonvolatile memory

30   component is not directly accessible via a system bus and access to the nonvolatile

31   memory component is limited to the custom logic block.

1   2.   (ORIGINAL) The system of claim 1 wherein the nonvolatile memory

2   component is isolated such that a system input/output module, microprocessor, or external

3   environment is prevented from direct access to the identification number.

1   3.   (ORIGINAL) The system of claim 1 wherein the identification number is

2   embedded after manufacturing.

1   4.   (ORIGINAL) The system of claim 1 wherein the custom logic block is

2   permitted to read the identification number.

1   5.   (ORIGINAL) The system of claim 4 wherein a function defined in the custom

2   logic block specifies an operation to be performed using the hidden identification number.

1   6.   (CURRENTLY AMENDED) The system of claim 1 further comprising a

2   onetime programmable memory protected by a hardware fuse that isolates the identification

3   number from the-a microprocessor after the identification number is written.

1   7.   (ORIGINAL) The system of claim 1 wherein the custom logic block is

2   configured to embed the identification number into the nonvolatile memory component.

1   8.   (ORIGINAL) The system of claim 1 further comprising a microprocessor that

2   is configured to embed the identification number into the nonvolatile memory component.

1   9.   (ORIGINAL) The system of claim 1 wherein access to the digital services is

2   rejected when the hidden non-modifiable identification number is on a list of unauthorized

3   identification numbers.

3

1   10. (CURRENTLY AMENDED) A method for limiting unauthorized access to

2 digital services comprising:

3   (a) embedding a hidden non-modifiable identification number into a nonvolatile

4 memory component, wherein:

5   (i) the nonvolatile memory component is used to contain state information

6   to provide desired functionality and enforce one or more security policies for accessing

7   the digital services;

8   (ii) the hidden non-modifiable identification number uniquely identifies a

9   device containing the nonvolatile memory component; and

10   (iii) access to the digital services is based on access rights associated with the

11   hidden non-modifiable identification number; and

12   (iv) the identification number is used to limit a cloning attack wherein said

13   cloning attack comprises copying the identification number to a new device; and

14   (b) isolating access to the nonvolatile memory component such that access to the

15 nonvolatile memory component is limited to a fixed state custom logic block, the nonvolatile

16 memory component is protected such that the nonvolatile memory component is read only, and

17 the nonvolatile memory component is not directly accessible via a system bus.

1   11. (ORIGINAL) The method of claim 10 wherein the nonvolatile memory

2 component is isolated by preventing a system input/output module, microprocessor, or external

3 environment from direct access to the identification number.

1   12. (ORIGINAL) The method of claim 10 wherein the identification number is

2 embedded after manufacturing.

1   13. (ORIGINAL) The method of claim 10 wherein the custom logic block is

2 permitted to read the identification number.

4

1   14.   (ORIGINAL) The method of claim 13 wherein a function defined in the

2   custom logic block specifies an operation to be performed using the hidden identification

3   number.

1   15.   (CURRENTLY AMENDED) The method of claim 10 wherein the

2   identification number is embedded using a onetime programmable memory protected by a

3   hardware fuse that isolates the identification number from the~~the~~ a_microprocessor after the

4   identification number is written.

1   16.   (ORIGINAL) The method of claim 10 wherein the custom logic block embeds

2   the identification number into the nonvolatile memory component.

1   17.   (ORIGINAL) The method of claim 10 wherein a microprocessor embeds the

2   identification number into the nonvolatile memory component.

1   18.   (ORIGINAL) The method of claim 10 further comprising rejecting access to

2   the digital services when the hidden non-modifiable identification number is on a list of

3   unauthorized identification numbers.

1   19.   (CURRENTLY AMENDED) A conditional access module (CAM), comprising:

2   (a)   a nonvolatile memory component, wherein:

3   (i)   the nonvolatile memory component is used to contain state information

4   to provide desired functionality and enforce one or more security policies for accessing

5   digital services; and

6   (ii)   the nonvolatile memory component is protected from modification such

7   that the nonvolatile memory component is read only; and

8   (iii)   access to the nonvolatile memory component is isolated;

9   (b)   a hidden non-modifiable identification number embedded into the nonvolatile

10 memory component, wherein:

11   (i)   -the identification number uniquely identifies the CAM; and

5

12   (ii)   the identification number is used to limit a cloning attack wherein said

13   cloning attack comprises copying the identification number to a new CAM; and

14   (c)   a fixed state custom logic block, wherein the nonvolatile memory component is

15   not directly accessible via a system bus and access to the nonvolatile memory component is

16   limited to the custom logic block.

1   20.   (ORIGINAL) The CAM of claim 19 wherein the nonvolatile memory

2   component is isolated such that a system input/output module, microprocessor, or external

3   environment is prevented from direct access to the identification number.

1   21.   (ORIGINAL) The CAM of claim 19 wherein the identification number is

2   embedded after manufacturing.

1   22.   (ORIGINAL) The CAM of claim 19 wherein the custom logic block is

2   permitted to read the identification number.

1   23.   (ORIGINAL) The CAM of claim 22 wherein a function defined in the custom

2   logic block specifies an operation to be performed using the hidden identification number.

1   24.   (CURRENTLY AMENDED) The CAM of claim 19 further comprising a

2   onetime programmable memory protected by a hardware fuse that isolates the identification

3   number from ~~the a~~ microprocessor after the identification number is written.

1   25.   (ORIGINAL) The CAM of claim 19 wherein the custom logic block is

2   configured to embed the identification number into the nonvolatile memory component.

1   26.   (ORIGINAL) The CAM of claim 19 further comprising a microprocessor that

2   is configured to embed the identification number into the nonvolatile memory component.

1   27.   (ORIGINAL) The CAM of claim 19 wherein access to the digital services is

2   rejected when the hidden non-modifiable identification number is on a list of unauthorized

3   identification numbers.

6

1   28.   (CURRENTLY AMENDED) An article of manufacture for limiting

2 unauthorized access to digital services comprising:

3   (a)   means for embedding a hidden non-modifiable identification number into a

4 nonvolatile memory component, wherein:

5   (i)   the nonvolatile memory component is used to contain state information

6   to provide desired functionality and enforce one or more security policies for accessing

7   the digital services;

8   (ii)   the hidden non-modifiable identification number uniquely identifies a

9   device containing the nonvolatile memory component; ~~and~~

10   (iii)   access to the digital services is based on access rights associated with the

11   hidden non-modifiable identification number; <u>and</u>

12   <u>(iv)   the identification number is used to limit a cloning attack wherein said</u>

13   <u>cloning attack comprises copying the identification number to a new device;</u> and

14   (b)   means for isolating access to the nonvolatile memory component such that

15 access to the identification number is limited to a fixed state custom logic block, the nonvolatile

16 memory component is protected from modification such that the nonvolatile memory

17 component is read only, and the nonvolatile memory component is not directly accessible via a

18 system bus.

1   29.   (ORIGINAL) The article of manufacture of claim 28 wherein the nonvolatile

2 memory component is isolated by preventing a system input/output module, microprocessor, or

3 external environment from direct access to the identification number.

1   30.   (ORIGINAL) The article of manufacture of claim 28 wherein the identification

2 . number is embedded after manufacturing.

1   31.   (ORIGINAL) The article of manufacture of claim 28 wherein the custom logic

2 block is permitted to read the identification number.

7

1   32.   (ORIGINAL) The article of manufacture of claim 31 wherein a function
2   defined in the custom logic block specifies an operation to be performed using the hidden
3   identification number.

1   33.   (CURRENTLY AMENDED) The article of manufacture of claim 28 wherein
2   the identification number is embedded using a onetime programmable memory protected by a
3   hardware fuse that isolates the identification number from the~a~microprocessor after the
4   identification number is written.

1   34.   (ORIGINAL) The article of manufacture of claim 28 wherein the custom logic
2   block embeds the identification number into the nonvolatile memory component.

1   35.   (ORIGINAL) The article of manufacture of claim 28 wherein a microprocessor
2   embeds the identification number into the nonvolatile memory component.

1   36.   (ORIGINAL) The article of manufacture of claim 28 further comprising means
2   for rejecting access to the digital services when the hidden non-modifiable identification number
3   is on a list of unauthorized identification numbers.

8